

Quantum Versus Classical Advantages in Secret Key Distillation (and Their Links to Quantum Entanglement)

Eric Chitambar¹, Ben Fortescue¹, Min-Hsiu Hsieh²

¹ *Department of Physics and Astronomy, Southern Illinois University,
Carbondale, Illinois 62901, USA*

² *Centre for Quantum Computation & Intelligent Systems (QCIS),
Faculty of Engineering and Information Technology (FEIT),
University of Technology Sydney (UTS), NSW 2007, Australia*

October 27, 2015

Abstract

We consider the extraction of shared secret key from correlations that are generated by either a classical or quantum source. In the classical setting, two honest parties (Alice and Bob) use public discussion and local randomness to distill secret key from some distribution p_{XYZ} that is shared with an unwanted eavesdropper (Eve). In the quantum settings, the correlations p_{XYZ} are delivered to the parties as either an *incoherent* mixture of orthogonal quantum states or as *coherent* superposition of such states; in both cases, Alice and Bob use public discussion and local quantum operations to distill secret key. While the power of quantum mechanics increases Alice and Bob's ability to generate shared randomness, it also equips Eve with a greater arsenal of eavesdropping attacks. Therefore, it is not obvious who gains the greatest advantage for distilling secret key when replacing a classical source with a quantum one.

In this paper we first demonstrate that the classical key rate is equivalent to the quantum key rate when the correlations are generated incoherently in the quantum setting. For coherent sources, we next show that the rates are incomparable, and in fact, their difference can be arbitrarily large in either direction. However, we identify a large class of non-trivial distributions p_{XYZ} that possess the following properties: (i) Eve's advantage is always greater in the quantum source than in its classical counterpart, and (ii) for the quantum entanglement shared between Alice and Bob in the coherent source, the so-called entanglement cost/squashed entanglement/relative entropy of entanglement can all be computed. With property (ii), we thus present a rare instance in which the various entropic entanglement measures of a quantum state can be explicitly calculated.

1 Introduction

When possessing a shared secret key, two parties can communicate over a public communication channel in a provably secure manner. Specifically, by using the key for a one-time pad encryption, the public message can faithfully encode the secret message, thereby protecting it from any eavesdropping third party. While it is impossible to establish secret key using public communication alone, it turns out that public communication can often be used to transform partially secret key into a stronger, more usable form, a process known as *secret key agreement* or *secret key distillation* [Mau93, AC93]. More precisely, suppose that the two parties (called Alice and Bob) share correlated random variables X and Y , but an eavesdropper (called Eve) has partial knowledge contained in her variable Z . Using public communication and local processing of their variables,

Alice and Bob may be able to generate a highly correlated pair of variables (\hat{X}, \hat{Y}) that is strongly uncorrelated with both Z and the conducted public communication, i.e. secret key.

Typically one considers the scenario where Alice, Bob, and Eve have access to some source that generates identical and independent copies of XYZ . The figure of merit then becomes the *secret key rate*, which is the largest number of secret bits per copy that Alice and Bob can obtain using local processing and public communication. Clearly if Z is highly correlated with either X or Y , then it will be impossible for key to be generated, even in the many-copy setting. But it is a significant open problem to understand precisely how Eve's side information Z affects the key rate.

There are a variety of physical situations in which one might encounter a many-copy source of variables XYZ . Most notably is the task of quantum key distribution (QKD) in which the variables XYZ are generated through the inherently stochastic nature of quantum measurement [BB84]. Alice, Bob, and Eve share a tripartite quantum state of the form $|\Psi\rangle^{ABE} = \sum_{x,y,z} e^{i\varphi_{xyz}} \sqrt{p(x,y,z)} |xyz\rangle^{ABE}$, where φ_{xyz} are arbitrary phases and $p(x,y,z)$ describes a joint distribution for variables XYZ . When the three parties measure their quantum system in the computational basis (i.e. in the $\{|x\rangle^A\}$, $\{|y\rangle^B\}$, and $\{|z\rangle^E\}$ basis respectively), their measurement outcomes are distributed according to $p(x,y,z)$. If this is done on multiple copies of $|\Psi\rangle^{ABE}$, the parties thus generate a many-copy source of XYZ from which Alice and Bob can distill secret key using public discussion and local processing.

Note that the described scenario only describes one particular way that Alice and Bob could use multiple copies of $|\Psi\rangle^{ABE}$ to obtain key. With quantum mechanics, more physical operations are allowed than just measuring in the computational basis. They could, for instance, put their local subsystems through some quantum channel (i.e. a trace-preserving, completely positive map), or they could each entangle their local subsystems and subject them to some joint unitary evolution before measuring. Naively then, it appears that with such greater operational powers, Alice and Bob can always distill at least as much key from a quantum source of $|\Psi\rangle^{ABE}$ than from a classical source of the underlying random variables XYZ . However, in the quantum scenario, Eve also gains operational strength in her eavesdropping abilities. This begs the natural question: for the purpose of secret key distillation, who gains the greatest advantage when embedding a given distribution $p(x,y,z)$ into a multi-party quantum system, the honest parties or the adversary?

Answering this question is the central aim of this paper. Through the construction of specific examples, we show that the advantage can lie either with Alice/Bob or with the Eve. Hence the adage "quantum is more powerful than classical" is really a matter of perspective when it comes to the task of secret key distillation. Furthermore, we prove that *quantum coherence* plays the essential role in affecting whether the quantum key rate differs from its classical counterpart. More precisely, in the state $|\Psi\rangle^{ABE}$ given above, the distribution $p(x,y,z)$ is encoded as a coherent superposition of the basis states $|xyz\rangle^{ABE}$. An alternative form of quantum embedding is an *incoherent* mixture of states $\rho^{ABE} = \sum_{x,y,z} p(x,y,z) |xyz\rangle\langle xyz|$. We prove that even when Alice and Bob are allowed to perform arbitrary quantum processing on their respective parts of ρ^{ABE} , their optimal rate of key extraction is not improved over the corresponding classical key rate. This result is significant as it identifies quantum coherence as precisely the ingredient that distinguishes classical from quantum secret key distillation, something that has not previously been understood.

Our second main result involves computing the entanglement of a quantum state based on the properties of its embedded classical distribution. Evaluating some of the most important entanglement measures for a general quantum state is a notoriously difficult problem due to the variational character of these measures. However, as we will demonstrate in this paper, when embedding quantum states with certain types of probability distributions, the entanglement can

be bounded by the secret key rate of the underlying distribution; and in some cases the two are equivalent. This offers a remarkable demonstration of how cryptographic results in classical information can be used to uncover novel physical properties of quantum systems.

The structure of this paper is as follows. In Sec. 2, we briefly summarize the main results of the paper. We then move to Sec. 3 where a relatively self-contained overview of the necessary concepts are present. In particular, we describe a unified framework for local information processing and public communication in both classical and quantum key distillation protocols. Secret key is presented as a classical analog to quantum entanglement, and the tasks of secret key distillation/formation are described as the counterparts to entanglement distillation/formation. While still in Sec. 3, we define classes of probability distributions that possess special properties such as the ability to dilute and compress secret correlations at equal rates. Main results and their proofs are collected in Sec. 4.

2 Summary of Results

We now summarize our results in two tables. The first describes classical versus quantum key rates K_D . The underlying classical distribution is p_{XYZ} and $|\Psi_{qqq}\rangle$ is its coherent embedding in a tripartite state. When one or more of the parties dephases in the computational basis, it generates a mixed state, and in this state we make the notational change $q \rightarrow c$ for the corresponding parties who dephase. Thus ρ_{ccc} is a full incoherent mixture according to the classical distribution p_{XYZ} . For completion we note a result given by Christandl *et. al* who showed a distribution p_{XYZ} for which Eve being quantum gives her a definite increase in power $K_D(\rho_{ccc}) > K_D(\rho_{ccq})$ [CEH⁺07].

Our second series of results involves analyzing the quantum versus classical rates for special classes of distributions. Details of these classes are presented in Sect 3, and here we just state the results. Most notably are the distributions possessing so-called secrecy reversibility, which can be shown to have the following property related to quantum versus classical advantages.

Theorem 1. *If a distribution p_{XYZ} possess secrecy reversibility, then Alice and Bob can gain no advantage over Eve when embedding their correlations into a quantum source (i.e. $K_D(p_{XYZ}) \geq K_D(\Psi_{qqq})$).*

It turns out that for a special subclass of reversible distributions, which also belong to the family of so-called semi-unambiguous distributions, we are able to compute the quantum entanglement in the embedded state. Specifically, the squashed entanglement (E_{sq}), the relative entropy of entanglement (E_r), and the entanglement of formation (E_F) can all be computed. This is remarkable since all previous calculations of these measures for a given mixed state involve exploring certain symmetries of the state (such as the so-called quantum flower states [CW05]). Our results are obtained purely by relating entanglement to the classical problem of secrecy reversibility. Our

| Rates | Results Presented Here |
|---|---|
| $K_D(p_{XYZ})$ vs. $K_D(\rho_{ccc})$ | $K_D(p_{XYZ}) = K_D(\rho_{ccc})$ |
| $K_D(p_{XYZ})$ vs. $K_D(\Psi_{qqq})$ | no general relationship with arbitrarily large gaps existing in both directions |
| $K_D(\rho_{ccq})$ vs. $K_D(\rho_{cqq})$ vs. $K_D(\rho_{qqq})$ | $K_D(\rho_{ccq}) \leq K_D(\rho_{cqq}) \leq K_D(\rho_{qqq})$ with arbitrarily large gaps existing between the rates |

Table 1: Quantum Versus Classical Advantages in Secret Key Distillation.

results are summarized in Table 2, where the quantity $J_{XY|Z}$ is the conditional common information .

3 Preliminary

3.1 A Unified Framework for Local Information Processing and Public Communication

In this section we review the definitions of classical and quantum local operations and public communication (LOPC).

3.1.1 Classical Operations.

In the classical LOPC setting, each party is allowed to perform the following operations:

- (i) Generate local random variables that are uncorrelated from the variables held by any other party.
- (ii) Generate copies of any locally held variables.
- (iii) Change the values of any locally held variables according to some function.
- (iv) Broadcast the result of any computed function over an authenticated public channel.

Note that operations (i) - (iii) encompass any sort of noisy processing that a party may wish to perform. A general **classical LOPC protocol** \mathcal{P}_c then consists of two phases: Phase I - a coordinated and multi-round exchange of public messages in which each message is a function of some party's local variables, and Phase II - each party processes his/her variables through a local channel chosen according to the messages of Phase I, thereby generating the output variables of the protocol. It is not difficult to see that the variables generated by any sequence of operations (i)–(iv) can always also be generated by a protocol following this two-phase format [AC93, Mau93, CK11].

Consider now an arbitrary random variable G that is distributed according to p_G over alphabet \mathcal{G} . Formally, we will represent G as a quantum state:

$$\omega_G = \sum_{g \in \mathcal{G}} p(g) |g\rangle\langle g|, \quad (1)$$

| Type of Distribution | Results Presented Here |
|--|--|
| Secrecy Reversible | $K_D(p_{XYZ}) \geq E_{sq}(\rho^{AB})$ |
| Secrecy Reversible + UBI-PD | $K_D(p_{XYZ}) \geq E_F(\rho^{AB})$ |
| Secrecy Reversible + Semi-unambiguous | $K_C(p_{XYZ}) = E_{sq}(\rho^{AB}) = K_D(\Psi^{ABE}) = K_D(p^{XYZ})$ |
| Secrecy Reversible + UBI-PD + Semi-Unambiguous | $K_C(p_{XYZ}) = E_F(\rho^{AB}) = E_C(\rho^{AB}) = E_{sq}(\rho^{AB}) = E_r(\rho^{AB})$ $= E_D(\rho^{AB}) = K_D(\Psi^{ABE}) = K_D(p_{XYZ}) = H(J_{XY Z} Z)$ |

Table 2: Linking secret keys to quantum entanglement.

where the $|g\rangle$ are orthonormal vectors for a vector space of dimension $|\mathcal{G}|$. When ω_G is subjected to classical operations (i)–(iv), it will transform as

$$\begin{aligned}
\omega_G &\xrightarrow{(i)} \omega_G \otimes \omega_S^{\text{local}} \quad \text{for local ancillary variable } S; \\
\omega_G &\xrightarrow{(ii)} \sum_{g \in \mathcal{G}} p(g) |g\rangle\langle g| \otimes |g\rangle\langle g|^{\text{local}}; \\
\omega_G &\xrightarrow{(iii)} \sum_{g \in \mathcal{G}} p(g) |f(g)\rangle\langle f(g)|^{\text{local}} \\
\omega_G &\xrightarrow{(iv)} \sum_{g \in \mathcal{G}} p(g) |g\rangle\langle g| \otimes |f(g)\rangle\langle f(g)|^{\text{global}}.
\end{aligned} \tag{2}$$

Here, “local” (resp. “global”) refers to some system storing classical information which only one party (resp. all parties) can access.

3.1.2 Quantum Operations.

In the quantum LOPC setting, each party is allowed to perform the following operations:

- (i) Perform a local quantum instrument $(\mathcal{E}_m)_m$ [DL70], where each \mathcal{E}_m is a completely positive (CP) map, and their sum $\sum_m \mathcal{E}_m$ is a trace-preserving map. Quantum instruments represent the most general type of quantum measurement. When performing the instrument on the state σ , the “measurement” outcome m is obtained with probability $p(m) = \text{tr}[\mathcal{E}_m(\sigma)]$, and the post-measurement state given this outcome is $\sigma_m = \mathcal{E}_m(\sigma) / p(m)$.
- (ii) Broadcast the result of any quantum measurement.

A general **quantum LOPC protocol** \mathcal{P}_q is described by a multi-level “tree” of local instruments in which the choice of instrument performed at each node of the tree depends on the particular history of measurement outcomes leading up to that node (see Ref. [KKB11, CH14, CLM⁺14] for details). Transformations (i)–(iii) in Eq. (2) fall within the framework of local quantum instruments since evaluating a function is a special type of quantum measurement in which the measurement outcome is the function’s value. Therefore, quantum LOPC generalizes the notion of classical LOPC.

With a slight abuse of notation, for a given classical/quantum protocol we use $\mathcal{P}_c / \mathcal{P}_q$ to denote both the particular protocol as well as the map associated with the protocol:

$$\mathcal{P}(\sigma^{ABE}) = \sum_m p(m) \sigma_m^{ABE} \otimes |m\rangle\langle m|^{\text{global}},$$

where σ_m^{ABE} is the tripartite state generated when m is the total broadcasted message. The random variable associated with the global communication is

$$\omega_M^{\text{global}} = \sum_m p(m) |m\rangle\langle m|^{\text{global}}.$$

3.2 A Classical versus quantum source of correlations

Throughout this paper, we will assume that some basis for Alice, Bob, and Eve’s system has been chosen and is fixed. Each of these is typically referred to as the *computational basis* for the given system and

is denoted by $\{|x\rangle^A\}_{x=1}^{d_A}$, $\{|y\rangle^B\}_{y=1}^{d_B}$ and $\{|z\rangle^E\}_{z=1}^{d_E}$ respectively. Let p_{XYZ} be an arbitrary three-way joint probability distribution for random variables X , Y , and Z which takes on values $p(x, y, z)$. We introduce the following physical instantiations of p_{XYZ} :

- A coherent embedding (or qqq embedding):

$$|\Psi_{qqq}\rangle = \sum_{x,y,z} e^{i\phi_{xyz}} \sqrt{p(x,y,z)} |xyz\rangle^{ABE}, \quad (3)$$

$$\text{for any } \phi_{xyz} \in [0, 2\pi). \quad (4)$$

- A one-sided incoherent embedding (or cqq embedding):

$$\rho_{cqq} = \sum_x p(x) |x\rangle\langle x|^A \otimes |\psi_x\rangle\langle\psi_x|^{BE}, \quad (5)$$

$$\text{where } |\psi_x\rangle = \sum_{y,z} e^{i\phi_{xyz}} \sqrt{p(y,z|x)} |yz\rangle.$$

- A two-sided incoherent embedding (or ccq embedding):

$$\rho_{ccq} = \sum_{x,y} p(x,y) |xy\rangle\langle xy|^{AB} \otimes |\psi_{xy}\rangle\langle\psi_{xy}|^E, \quad (6)$$

$$\text{where } |\psi_{xy}\rangle = \sum_z e^{i\phi_{xyz}} \sqrt{p(z|xy)} |z\rangle.$$

- An incoherent embedding (or ccc embedding):

$$\rho_{ccc} = \sum_{x,y,z} p(x,y,z) |xyz\rangle\langle xyz|^{ABE}. \quad (7)$$

Note that ρ_{ccc} corresponds to the state ω_{XYZ} introduced in Eq. (1). We can therefore think of ρ_{ccc} as either a classical or quantum object, the difference being dictated by whether it is processed using either classical or quantum LOPC.

Regardless of how the phases ϕ_{xyz} are chosen, the various embeddings can be related through a series of local physical transformations:

$$|\psi_{qqq}\rangle\langle\psi_{qqq}| \xrightarrow{(1)} \rho_{cqq} \xrightarrow{(2)} \rho_{ccq} \xrightarrow{(3)} \rho_{ccc}, \quad (8)$$

where (1) is attained by Alice performing a dephasing channel

$$\sigma \rightarrow \sum_x |x\rangle\langle x| \sigma |x\rangle\langle x|$$

and likewise for (2) and (3). It is also worth pointing out that since we allow for phases ϕ_{xyz} in the coherent superposition of Eq. (3), *any tripartite pure state can be regarded as the qqq state of some distribution*. This distribution p_{XYZ} is obtained simply by all three parties dephasing in the computational basis as shown in Eq. (8). Our approach is thus more general to previous studies in coherent embeddings [CEH⁺07], where it is typically assumed that $\phi_{xyz} = 0$ for all x, y , and z .

3.2.1 Secret Key Distillation.

The scenario we consider is an identical, independent, and discrete (i.i.d.) source that is generating some particular embedding of p_{XYZ} for Alice, Bob and Eve. The goal of Alice and Bob is to distill secret key, which is shared randomness held independently of Eve's system. We denote the state corresponding to $r := \log s$ bits of perfectly shared randomness by

$$\Phi_r^{AB} = \frac{1}{s} \sum_{i=1}^s |ss\rangle\langle ss|^{AB}. \quad (9)$$

The notion of secret key rate is defined as follows.

Definition 1. For distribution p_{XYZ} , we say that R is an **LOPC achievable key rate** if for every $\epsilon > 0$, there exists a classical LOPC protocol \mathcal{P}_c acting on $\sigma^{ABE} := \rho_{ccc}^{\otimes n}$ (for n sufficiently large) and generating messages ω_M^{global} such that

$$\left\| \mathcal{P}_c(\sigma^{AB}) - \Phi_{\lfloor nR - \epsilon \rfloor}^{AB} \otimes \left(\omega_M^{\text{global}} \otimes \sigma^E \right) \right\|_1 < \epsilon, \quad (10)$$

where $\sigma^{AB} = \text{tr}_E \sigma^{ABE}$ and $\sigma^E = \text{tr}_{AB} \sigma^{ABE}$. The supremum achievable key rate is denoted by $K_D(p_{XYZ})$. We say that R is a **ccc, ccq, cq, or qq LOPC achievable rate** if there exists a quantum LOPC protocol \mathcal{P}_q to replace \mathcal{P}_c in Eq. (10), and we further take $\sigma^{ABE} := \rho_{ccc}^{\otimes n}$, $\sigma^{ABE} := \rho_{ccq}^{\otimes n}$, $\sigma^{ABE} := \rho_{cq}^{\otimes n}$ or $\sigma^{ABE} := |\psi_{qqq}\rangle\langle\psi_{qqq}|^{\otimes n}$ respectively. The supremum achievable key rates in these scenarios are denoted by $K_D(\rho_{ccc})$, $K_D(\rho_{ccq})$, $K_D(\rho_{cq})$ and $K_D(\psi_{qqq})$ respectively.

3.3 Quantum Entanglement

Quantum entanglement is a resource shared between two or more quantum systems that is distinct from secret key [HHH09]. Starting from a tripartite pure state $|\Psi_{qqq}\rangle$, Alice and Bob share one entangled bit (ebit) of quantum information in the state $|\Psi_{qqq}\rangle$ if it has the form

$$|\Psi_{qqq}\rangle^{ABE} = |\Phi_2\rangle^{AB} \otimes |\varphi\rangle^E, \quad (11)$$

where $|\Phi_2\rangle^{AB} := \sqrt{1/2}(|00\rangle + |11\rangle)^{AB}$ is a so-called ebit and $|\varphi\rangle^E = \sum_z e^{i\varphi_z} \times \sqrt{p(z)}|z\rangle$ is any state held by Eve. On the surface, the tripartite state $|\Psi_{qqq}\rangle^{ABE} = |\Phi_2\rangle^{AB} \otimes |\varphi\rangle^E$ looks very similar to the state $\rho_{ccq}^{ABE} = \Phi_2^{AB} \otimes |\varphi\rangle\langle\varphi|^E$, which contains one bit distillable secret key and is obtained from $|\Psi_{qqq}\rangle^{ABE}$ through dephasing by Alice and Bob. However there is a critical difference between the two states. For $\Phi_2^{AB} \otimes |\varphi\rangle\langle\varphi|^E$, it is entirely consistent that there should exist some third party Sapna (S) who holds as side information the value of Alice and Bob's bit in Φ_2^{AB} . In other words, we can envision a four-party state $\sigma^{ABES} = \Phi_3^{ABS} \otimes |\varphi\rangle\langle\varphi|^E$ with $\Phi_3^{ABS} = \frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$. And while $K_D(\sigma^{ABE}) = 1$, there is no secrecy with respect to Sapna: $K_D(\sigma^{ABS}) = 0$. In contrast, Alice and Bob's entanglement in $|\Psi_{ABE}\rangle$ exists regardless of what side information is known. That is, if $\text{tr}_{ES}(\sigma^{ABES}) = |\Phi_2\rangle\langle\Phi_2|^{AB}$ for any state σ^{ABES} , then necessarily σ^{ABES} has the product-state form $\sigma^{ABES} = |\Phi_2\rangle\langle\Phi_2|^{AB} \otimes \sigma^{ES}$. This means that if Alice and Bob should dephase when holding the state σ^{ABES} , they will generate key that is secret from not only Eve but also Sapna: $|\Phi_2\rangle\langle\Phi_2|^{AB} \otimes \sigma^{ES} \rightarrow \Phi_2^{AB} \otimes \sigma^{ES}$. Therefore, entanglement is a property of a bipartite ρ^{AB} itself and, unlike secret key, one does not need to introduce any third party to speak of its entanglement.

Similar to the secret key rate K_D , one can also define for ρ^{AB} the entanglement distillation rate E_D [Rai99]. This quantifies the asymptotic rate for which ebits can be obtained from ρ^{AB} using

local operations and classical communication (LOCC). The operational class LOCC differs from quantum LOPC in that the former makes no explicit reference to a third party who records the “public” communication. It is a fundamental and challenging problem in quantum information to compute $E_D(\rho^{AB})$ for a given quantum state. Almost all meaningful measures of entanglement provide an upper bound for E_D [HHHO09], and three such measures are the relative entropy of entanglement [VP98], the squashed entanglement [CW04], and the entanglement of formation [BDSW96]:

- $E_r(\rho^{AB})$: the relative entropy of entanglement is

$$E_r(\rho^{AB}) = \min_{\sigma \in \mathcal{S}} S(\rho \| \sigma), \quad (12)$$

where \mathcal{S} is the set of separable density operators and $S(\rho \| \sigma) = -\text{tr}[\rho \log \sigma] - S(\rho)$ is the relative entropy;

- $E_{sq}(\rho^{AB})$: the squashed entanglement is

$$E_{sq}(\rho^{AB}) = \frac{1}{2} \inf_{\rho^{ABE}} I(A : B|E)_{\rho^{ABE}}, \quad (13)$$

where the infimum is taken over all extensions ρ^{ABE} such that $\text{Tr}_E \rho^{ABE} = \rho^{AB}$, and $I(A : B|E)_{\rho^{ABE}} = S(AE) + S(BE) - S(ABE) - S(E)$ is the conditional quantum mutual information of the state ρ^{ABE} .

- $E_F(\rho^{AB})$: the entanglement of formation is

$$E_F(\rho^{AB}) = \min \sum_i p(i) S(\text{Tr}_A \varphi_i), \quad (14)$$

with the minimization taken over all decompositions $\rho^{AB} = \sum_i p(i) |\varphi_i\rangle\langle\varphi_i|$.

The particular significance of these entanglement measures is that they provide upper bounds not only for the distillable entanglement but also for distillable key.

Theorem 2 ([HHHO05, HHHO09, Chr06]). *For an arbitrary tripartite state $|\Psi_{qqq}\rangle^{ABE}$ with $\rho^{AB} = \text{tr}_E |\Psi_{qqq}\rangle\langle\Psi_{qqq}|^{ABE}$, the rates $K_D(\Psi_{qqq})$ and $E_D(\rho^{AB})$ are both upper bounded by the relative entropy of entanglement $E_r(\rho^{AB})$ as well as the squashed entanglement $E_{sq}(\rho^{AB})$.*

Unfortunately, each of the above entanglement measures involves a complicated minimization and in fact, their evaluation represents an NP-hard/NP-complete computational problem [Hua14]. It is therefore not surprising that very few instances are known in which any of these measures can be explicitly computed. In this paper, we introduce a new class of quantum states for which all these measures can be evaluated. Our strategy will be based on the notion of *reversible secrecy*, which we describe next.

3.4 Reversible Entanglement and Secret Key

Dual to the task of entanglement distillation is the task of entanglement formation, which describes building a given state ρ^{AB} using LOCC and an initial supply of ebits. The **entanglement cost** E_C of a mixed state ρ^{AB} is the asymptotic optimal rate of ebit consumption for Alice and Bob to generate faithful copies of ρ^{AB} by LOCC [HHT01]. The entanglement cost is obviously lower

bounded by the distillable entanglement, and compared to the above entanglement measures, the following hierarchy holds [HHO09]:

$$\begin{cases} E_D(\rho^{AB}) \\ K_D(\Psi_{qqq}) \end{cases} \leq \begin{cases} E_r(\rho^{AB}) \\ E_{sq}(\rho^{AB}) \end{cases} \leq E_C(\rho^{AB}) \leq E_F(\rho^{AB}), \quad (15)$$

where the first inequality references Theorem 2. A state ρ^{AB} is said to possess **reversible entanglement** if $E_D(\rho^{AB}) = E_C(\rho^{AB})$. Operationally this means that the entanglement in ρ^{AB} can be concentrated and diluted at equal rates.

Recently, the phenomenon of **reversible secrecy**, which is the classical analog to reversible entanglement, was studied in [CFH15a]. Here, one first identifies the key cost K_C of a distribution p_{XYZ} as the amount of secret correlations needed for Alice and Bob to asymptotically prepare p_{XYZ} using classical LOPC [RW03]. The distribution is said to possess reversible secrecy if $K_D(p_{XYZ}) = K_C(p_{XYZ})$. A key result that we prove in Theorem 6 is that when p_{XYZ} is a reversible distribution and $|\Psi_{qqq}\rangle$ is a qqq embedding, then Eq. (15) can be further upper bounded as

$$\begin{cases} E_D(\rho^{AB}) \\ K_D(\Psi_{qqq}) \end{cases} \leq \begin{cases} E_r(\rho^{AB}) \\ E_{sq}(\rho^{AB}) \end{cases} \leq E_C(\rho^{AB}) \leq E_F(\rho^{AB}) \leq K_D(p_{XYZ}). \quad (16)$$

By identifying a class of distributions in Section 3.5 for which $K_D(\Psi_{qqq}) = K_D(p_{XYZ})$, this chain of inequalities becomes tight and we are thus able to compute the various entanglement measures of ρ^{AB} .

3.5 Classes of Classical Distributions Related to Secrecy Reversibility

For a tripartite distribution p_{XYZ} , we can define *maximal conditional common function* $J_{XY|Z} = \{J_{XY|Z=z} : p_Z(z) > 0\}$, where $J_{XY|Z=z}$ is the common information of a bipartite distribution $P_{XYZ}(x, y|Z = z)$ [GK73]. For completeness, we provide a self-contained introduction of $J_{XY|Z}$ in Appendix 6.1.

A distribution p_{XYZ} is said to be ([CFH15b, CFH15a]):

- **Block independent** (BI) if $I(X : Y|J_{XY|Z}Z) = 0$.
- **Uniform block independent** (UBI) if both $I(X : Y|J_{XY|Z}Z) = 0$ and $H(J_{XY|Z}|X) = H(J_{XY|Z}|Y) = 0$.
- **Uniform block independent under public discussion** (UBI-PD) if it is BI and there is a public communication protocol generating messages M such that $p_{(MX)(MY)(ZM)}$ is UBI and $I(M : J_{XY|Z}|Z) = 0$.
- **Uniform block independent under public discussion and eavesdropper's local processing** (UBI-PD_↓) if there exists a channel $\bar{Z}|Z$ such that $p_{XY|\bar{Z}}$ is UBI with the required public communication M also satisfying $I(Z : J_{XY|\bar{Z}}|M\bar{Z}) = 0$.
- **Semi-unambiguous** [CEH⁺07] if $H(Z|XY) = 0$.
- **Unambiguous** [OSS14] if $H(Z|XY) = 0$ and $H(XY|J_{XY|Z}Z) = 0$.

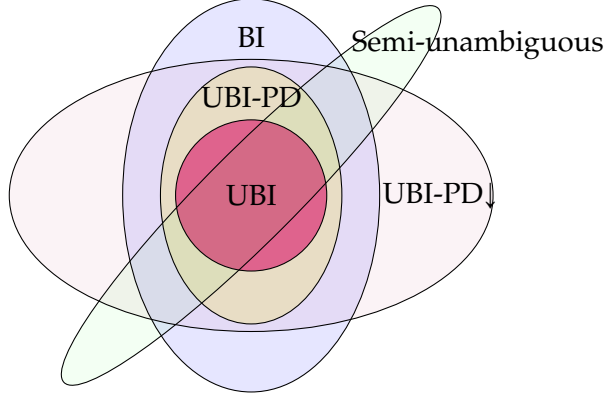


Figure 1: The relations between known classical distributions.

The relations between these distributions are depicted in Figure 1.

Being BI means that given Z , Alice and Bob share no more correlations besides their block number given by some maximal common function $J_{XY|Z}$. For UBI distributions, the block number is independent of Z and can therefore be computed locally by Alice and Bob. Finally, for UBI-PD, the distribution becomes UBI once Alice shares with Bob her and Eve's common information, and Bob does likewise. Of course, Eve learns nothing new about XY through this public discussion. For semi-unambiguous distributions, the random variable Z can be uniquely determined by random variables X and Y ; while for unambiguous distributions, each random variable can be uniquely determined by the other two random variables.

The significance of these distributions to the problem of secrecy reversibility is given in the following theorem.

Theorem 3 ([CFH15a]). (1) If $K_C(p_{XYZ}) = K_D(p_{XYZ})$ then there exists a channel for Eve $\bar{Z}|Z$ such that $p_{XY\bar{Z}}$ is BI. (2) If p_{XYZ} is UBI-PD \downarrow , then $K_C(p_{XYZ}) = K_D(p_{XYZ})$.

In Ref. [CFH15a], it is shown that the necessary condition (1) and sufficient condition (2) are equivalent whenever either Alice or Bob holds a binary random variable.

4 Main Results and Proofs

4.1 Advantages in Quantum versus Classical Key Distillation

4.1.1 No advantages in incoherent embeddings.

Theorem 4. $K_D(p_{XYZ}) = K_D(\rho_{ccc})$ for any distribution p_{XYZ} .

Proof. The inequality $K_D(\rho_{ccc}) \geq K_D(p_{XYZ})$ is immediate from the fact every classical protocol \mathcal{P}_c is a special type of quantum protocol \mathcal{P}_q . Now we turn to the converse $K_D(\rho_{ccc}) \geq K_D(p_{XYZ})$. The idea will be to show that every quantum LOPC protocol \mathcal{P}_q distilling secret key can be transformed into a classical protocol \mathcal{P}_c that distills the same amount of key. Suppose that $\|\mathcal{P}_q(\rho_{ccc}^{\otimes n}) - \Phi_s^{AB} \otimes (\omega_M^{\text{global}} \otimes \sigma^E)\| < \epsilon$ with $\sigma^E = \text{tr}_{AB}(\rho_{ccc}^{\otimes n})$ and \mathcal{P}_q some r -round quantum LOPC protocol. To perform the following analysis let's fix some notation. First, without loss of generality, let's assume that r is even with Alice (resp. Bob) measuring in all the odd-numbered (resp. even-numbered) rounds. We let $i_{\leq k}$ denote a particular sequence of the first k rounds with $i_{< k} := i_{\leq k-1}$. If we wish

to refer to a specific outcome in the k^{th} round, we will denote this by i_k . Hence $i_{\leq k} = (i_1, i_2, \dots, i_k)$ for some particular sequence. Finally, if, say, Alice is the measuring party in the k^{th} round, we denote her local instrument conditioned on outcome $i_{<k}$ by $(\mathcal{A}_{i_k}^{(i_{<k})})_{i_k}$. If we wish to speak of the full composition of Alice's CP maps corresponding to the outcome sequence $i_{\leq k}$, we will denote this simply by $\mathcal{A}^{(i_{\leq k})}$, with no subscript. That is (for odd-numbered k) we have

$$\mathcal{A}^{(i_{\leq k})} = \mathcal{A}_{i_k}^{(i_{<k})} \circ \mathcal{A}^{(i_{\leq k-2})} = \mathcal{A}_{i_k}^{(i_{<k})} \circ \mathcal{A}_{i_{k-2}}^{(i_{<k-2})} \circ \dots \circ \mathcal{A}_{i_1},$$

and similarly Bob's action is described by

$$\mathcal{B}^{(i_{\leq k-1})} = \mathcal{B}_{i_{k-1}}^{(i_{<k-1})} \circ \mathcal{B}^{(i_{\leq k-3})} = \mathcal{B}_{i_{k-1}}^{(i_{<k-1})} \circ \mathcal{B}_{i_{k-3}}^{(i_{<k-3})} \circ \dots \circ \mathcal{B}_{i_2}^{(i_1)}.$$

With the notation in hand, when performing protocol \mathcal{P}_q on $\rho_{ccc}^{\otimes n}$, we can describe the overall state of generated across all outcome branches by

$$\begin{aligned} & \mathcal{P}_q(\rho_{ccc}^{\otimes n}) \\ &= \sum_{\mathbf{x}, \mathbf{y}, \mathbf{z}} \sum_{i_{\leq r}} p^n(\mathbf{x}, \mathbf{y}, \mathbf{z}) \quad \mathcal{A}^{(i_{\leq r-1})} \otimes \mathcal{B}^{(i_{\leq r})} (|\mathbf{x}\mathbf{y}\rangle\langle\mathbf{x}\mathbf{y}|) \otimes |\mathbf{z}\rangle\langle\mathbf{z}|^E \otimes |i_{\leq r}\rangle\langle i_{\leq r}|^{\text{global}}, \end{aligned} \quad (17)$$

where the first sum is over $\mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ with $p^n(\mathbf{x}, \mathbf{y}, \mathbf{z})$ being the n -fold product distribution of p_{XYZ} , and the second sum is over all possible measurement sequences. If Alice and dephase $\mathcal{P}_q(\rho_{ccc}^{\otimes n})$ in the computational basis, the resulting state will be at least ϵ -close to $\Phi_s^{AB} \otimes (\omega_M^{\text{global}} \otimes \sigma^E)$ by monotonicity of the trace norm. Hence it suffices to show that this dephased state $\Delta(\mathcal{P}_q(\rho_{ccc}^{\otimes n}))$ can be generated using classical LOPC. To see that this is possible, we repeatedly use the fact that the messages are generated locally to form the expansion

$$\begin{aligned} \Delta(\mathcal{P}_q(\rho_{ccc}^{\otimes n})) &= \sum_{\mathbf{x}', \mathbf{y}'} \sum_{\mathbf{x}, \mathbf{y}, \mathbf{z}} \sum_{i_{\leq r}} \Pr[\mathbf{x}', \mathbf{y}' | i_{\leq r}, \mathbf{x}, \mathbf{y}, \mathbf{z}] p^n(\mathbf{x}, \mathbf{y}, \mathbf{z}) \\ &\quad \cdot |\mathbf{x}'\mathbf{y}'\rangle\langle\mathbf{x}'\mathbf{y}'|^{AB} \otimes |\mathbf{z}\rangle\langle\mathbf{z}|^E \otimes |i_{\leq r}\rangle\langle i_{\leq r}|^{\text{global}} \end{aligned} \quad (18)$$

where

$$\Pr[\mathbf{x}', \mathbf{y}' | i_{\leq r}, \mathbf{x}, \mathbf{y}, \mathbf{z}] = \frac{\langle \mathbf{x}' | \mathcal{A}^{(i_{\leq r-1})} (|\mathbf{x}\rangle\langle\mathbf{x}|) | \mathbf{x}' \rangle \cdot \langle \mathbf{y}' | \mathcal{B}^{(i_{\leq r})} (|\mathbf{y}\rangle\langle\mathbf{y}|) | \mathbf{y}' \rangle}{\Pr[i_{\leq r} | \mathbf{x}, \mathbf{y}, \mathbf{z}]} \quad (19)$$

and

$$\begin{aligned} \Pr[i_{\leq r} | \mathbf{x}, \mathbf{y}, \mathbf{z}] &= \text{tr}[\mathcal{A}^{(i_{\leq r-1})} \otimes \mathcal{B}^{(i_{\leq r})} (|\mathbf{x}\mathbf{y}\rangle\langle\mathbf{x}\mathbf{y}|)] \\ &= \prod_{\text{even } k}^r \frac{\text{tr}[\mathcal{A}^{(i_{\leq k-1})} \otimes \mathcal{B}^{(i_{\leq k})} (|\mathbf{x}\mathbf{y}\rangle\langle\mathbf{x}\mathbf{y}|)]}{\text{tr}[\mathcal{A}^{(i_{\leq k-1})} \otimes \mathcal{B}^{(i_{\leq k-2})} (|\mathbf{x}\mathbf{y}\rangle\langle\mathbf{x}\mathbf{y}|)]} \\ &\quad \times \prod_{\text{odd } k}^r \frac{\text{tr}[\mathcal{A}^{(i_{\leq k})} \otimes \mathcal{B}^{(i_{\leq k-1})} (|\mathbf{x}\mathbf{y}\rangle\langle\mathbf{x}\mathbf{y}|)]}{\text{tr}[\mathcal{A}^{(i_{\leq k-2})} \otimes \mathcal{B}^{(i_{\leq k-1})} (|\mathbf{x}\mathbf{y}\rangle\langle\mathbf{x}\mathbf{y}|)]} \\ &= \prod_{\text{even } k}^r \frac{\text{tr}[\mathcal{B}^{(i_{\leq k})} (|\mathbf{y}\rangle\langle\mathbf{y}|)]}{\text{tr}[\mathcal{B}^{(i_{\leq k-2})} (|\mathbf{y}\rangle\langle\mathbf{y}|)]} \times \prod_{\text{odd } k}^r \frac{\text{tr}[\mathcal{A}^{(i_{\leq k})} (|\mathbf{x}\rangle\langle\mathbf{x}|)]}{\text{tr}[\mathcal{A}^{(i_{\leq k-2})} (|\mathbf{x}\rangle\langle\mathbf{x}|)]}. \end{aligned} \quad (20)$$

Thus a classical protocol \mathcal{P}_c generating $\Delta(\mathcal{P}_q(\rho_{ccc}^{\otimes n}))$ is the following:

1. In the first round, Alice measures her variable \mathbf{x} and broadcasts message i_1 with probability $Pr[i_1|\mathbf{x}] = tr[\mathcal{A}_{i_1}(|\mathbf{x}\rangle\langle\mathbf{x}|)]$.
2. In every subsequent even-numbered (resp. odd-numbered) round k , Bob (resp. Alice) consults the message history $i_{<k}$ and broadcasts i_k with probability

$$Pr[i_k|i_{<k}, \mathbf{y}] = \frac{tr[\mathcal{B}_{i_k}^{(i_{<k})} \circ \mathcal{B}^{(i_{\leq k-2})}(|\mathbf{y}\rangle\langle\mathbf{y}|)]}{tr[\mathcal{B}^{(i_{\leq k-2})}(|\mathbf{y}\rangle\langle\mathbf{y}|)]} \quad (21)$$

$$\left(\text{resp. } Pr[i_k|i_{<k}, \mathbf{x}] = \frac{tr[\mathcal{A}_{i_k}^{(i_{<k})} \circ \mathcal{A}^{(i_{\leq k-2})}(|\mathbf{x}\rangle\langle\mathbf{x}|)]}{tr[\mathcal{A}^{(i_{\leq k-2})}(|\mathbf{x}\rangle\langle\mathbf{x}|)]} \right). \quad (22)$$

3. At the end of r rounds with the total message $i_{\leq r}$ having been generated, Alice and Bob process their variables using local channels $\mathbf{x} \rightarrow \mathbf{x}'$ and $\mathbf{y} \rightarrow \mathbf{y}'$ with transition probabilities given by

$$Pr[\mathbf{x}'|i_{\leq r}, \mathbf{x}] = \frac{\langle \mathbf{x}' | \mathcal{A}^{(i_{\leq r})}(|\mathbf{x}\rangle\langle\mathbf{x}|) | \mathbf{x}' \rangle}{tr[\mathcal{A}^{(i_{\leq r})}(|\mathbf{x}\rangle\langle\mathbf{x}|)]}, \quad (23)$$

$$Pr[\mathbf{y}'|i_{\leq r}, \mathbf{y}] = \frac{\langle \mathbf{y}' | \mathcal{B}^{(i_{\leq r})}(|\mathbf{y}\rangle\langle\mathbf{y}|) | \mathbf{y}' \rangle}{tr[\mathcal{B}^{(i_{\leq r})}(|\mathbf{y}\rangle\langle\mathbf{y}|)]}. \quad (24)$$

4. It can be seen that the state generated through this process is precisely $\Delta(\mathcal{P}_q(\rho_{ccc}^{\otimes n}))$.

□

4.1.2 Arbitrarily large advantages in coherent embeddings.

Theorem 5. For any N , a distribution p_{XYZ} exists such that when embedding p_{XYZ} into a coherent quantum source, one of the following relationships holds:

- (a) Eve gains an arbitrarily large advantage: $K_D(p_{XYZ}) - K_D(\Psi_{qqq}^{ABE}) > N$, or
- (b) Alice and Bob gain an arbitrarily large advantage: $K_D(\Psi_{qqq}^{ABE}) - K_D(p_{XYZ}) > N$.

Remark. In the proof of (a) we actually demonstrate a much stronger result that $K_D(p_{XYZ}) - E_F(\rho^{AB}) > N$. This means that we can distill key from p_{XYZ} from a considerably higher rate than the rate of entanglement needed to generate the corresponding quantum state ρ^{AB} . To our knowledge, this is the first known result of its kind.

Proof. (a) We consider a very simple binary distribution with $p(0,0,0) = p(1,1,0) = 1/4$, $p(0,0,1) = \lambda/2$, and $p(1,1,1) = (1-\lambda)/2$. This is a UBI distribution and by Theorem 3 below, its key rate precisely $K_D(p_{xyz}) = [1 + h(\lambda)]/2$, where $h(x) = -x \log x - (1-x) \log(1-x)$. The corresponding qqq embedding has the form

$$|\Psi_{qqq}^{ABE}\rangle = \sqrt{1/2} [|\Phi\rangle^{AB}|0\rangle^E + (\sqrt{\lambda}|00\rangle + \sqrt{1-\lambda}|11\rangle)^{AB}|1\rangle^E].$$

Since ρ^{AB} is a two-qubit state, its entanglement of formation can be calculated using the celebrated concurrence formula [Woo98] (see also [CFH15a]), and it is found to be

$$E_F(\rho^{AB}) = h \left([1 + \sqrt{1 - \left(1 + \sqrt{\lambda(1-\lambda)}\right)^2}] / 2 \right).$$

A simple convexity argument shows that $K_D(p_{XYZ}) > E_F(\rho^{AB})$ whenever $0 < \lambda < 1/2$. We now consider n copies of p_{XYZ} . Inspection reveals that $p_{XYZ}^{\otimes n}$ is also UBI for any n . Thus, $K_D(p_{XYZ}) = n[1 + h(\lambda)]/2$. On the other hand, the entanglement of formation is a sub-additive quantity such that $E_F((\rho^{AB})^{\otimes n}) \leq nE_F(\rho^{AB})$. Consequently, for any $0 < \lambda < 1/2$ we attain an arbitrarily large gap between $K_D(p_{XYZ}^n)$ and $E_F((\rho^{AB})^{\otimes n})$. By Theorem 2 and the fact that $E_F(\rho^{AB}) \geq E_{sq}(\rho^{AB})$, this gap will be at least as large as the gap between $K_D(p_{XYZ}^n)$ and $K_D((\Psi_{qqq}^{ABE})^{\otimes n})$.

(b) Consider the state $|\Psi\rangle^{ABE} = \sqrt{1/2}(|00\rangle + |1+\rangle)^{AB}|0\rangle^E$ where Eve is initially uncorrelated. This is a qqq encoding of a distribution $p_{XYZ} = p_{XY} \cdot q_Z$ whose mutual information is $I(X : Y) = 1 - h(1/3) \approx .311$. Since Eve has no side information, the classical secret key rate $K_D(p_{XYZ})$ is equal to the mutual information, a well-known result in secret key agreement [Mau93, AC93]. On the entanglement side, the reduced-state entropy characterizes the entanglement distillation rate for pure states [BBPS96]; hence $S(\rho^B) = E_D(\Psi^{ABE})$. One bit of entanglement can be converted into one bit of secret key, and thus $K_D(\Psi^{ABE}) \geq S(\rho^B)$. In fact, this inequality is tight since $S(\rho^B) = E_{sq}(\Psi^{AB}) \geq K_D(\Psi^{ABE})$. Because both the mutual information and von Neumann entropy are additive, a similar argument to part (a) shows that the gap between $S((\rho^B)^{\otimes n}) - K_D(p_{XYZ})$ can be made arbitrarily large. \square

4.1.3 Advantages in one-sided versus two-sided coherent embeddings.

From Theorem 4, we see that the presence of quantum coherence is necessary for there to be a difference in quantum and classical key distillation. The next example extends this result to states in which only one of the subsystems has quantum coherence.

Lemma 1. *There exists states for which*

$$K_D(\Psi_{qqq}) > K_D(\rho_{cqq}) > K_D(\rho_{ccq}).$$

In fact, the gaps between these rates can be arbitrarily large.

Proof. Consider the qqq embedded state

$$|\Psi_{qqq}\rangle = \frac{1}{\sqrt{6}} \left([|00\rangle + |11\rangle] \otimes |0\rangle + [|+2\rangle + |-3\rangle] \otimes |1\rangle + [|2+\rangle + |3-\rangle] \otimes |2\rangle \right) \quad (25)$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. The two dephased states of interest are given by

$$\begin{aligned} \rho_{cqq} = & \frac{1}{3} \Phi_2^{AB} \otimes |0\rangle\langle 0|^E + \frac{1}{6} (|0\rangle\langle 0| + |1\rangle\langle 1|)^A \otimes (|2\rangle\langle 2| + |3\rangle\langle 3|)^B \otimes |1\rangle\langle 1|^E \\ & + \frac{1}{6} (|2+\rangle\langle 2+| + |3-\rangle\langle 3-|)^{AB} \otimes |2\rangle\langle 2|^E, \end{aligned} \quad (26)$$

$$\begin{aligned} \rho_{ccq} = & \frac{1}{3} \Phi_2^{AB} \otimes |0\rangle\langle 0|^E + \frac{1}{6} (|0\rangle\langle 0| + |1\rangle\langle 1|)^A \otimes (|2\rangle\langle 2| + |3\rangle\langle 3|)^B \otimes |1\rangle\langle 1|^E \\ & + \frac{1}{6} (|2\rangle\langle 2| + |3\rangle\langle 3|)^A \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)^B \otimes |2\rangle\langle 2|^E. \end{aligned} \quad (27)$$

From the squashed entanglement upper bound on K_D , we find that $K_D(\Psi_{qqq}) \leq 1$, $K_D(\rho_{cqq}) \leq 2/3$, and $K_D(\rho_{ccq}) \leq 1/3$. In fact, each of these bounds are tight using the following protocol. For instance, with the state $|\Psi_{qqq}\rangle$, Alice and Bob both perform a projection into the $\{|0\rangle, |1\rangle\}$ or $\{|2\rangle, |3\rangle\}$ subspace. If one of them indeed projects into $\{|2\rangle, |3\rangle\}$, then the other party dephases in

the $\{|+\rangle, |-\rangle\}$ basis. Finally, a local unitary rotation is made back to the $\{|0\rangle, |1\rangle\}$ basis for both parties. Doing so generates the state $\Phi_2^{AB} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|)^E / 3$. For ρ_{cqq} a similar protocol is performed except that no key is obtained when Bob projects into the $\{|2\rangle, |3\rangle\}$ subspace (which occurs with probability $1/3$). And for ρ_{ccq} , secret key is obtained with probability $1/3$ when both parties projection into the $\{|0\rangle, |1\rangle\}$ subspace. Note that for n copies, the upper bounds become $K_D(\Psi_{qqq}^{\otimes n}) \geq n$, $K_D(\rho_{cqq}^{\otimes n}) \geq 2/3n$, and $K_D(\rho_{ccq}^{\otimes n}) \geq 1/3n$, which again are all tight. So by considering many copies, we obtain examples where the gap between the different key rates is arbitrarily large. \square

4.2 Embedding Distributions with Reversible Secrecy

We now consider qqq embeddings of distributions with reversible secrecy, for which it turns out that the quantum embedding favours Eve over Alice and Bob. When adding UBI-PD and/or semi-unambiguous structure, relationships between key and quantum entanglement can be drawn.

Theorem 6. (a) If p_{XYZ} has reversible secrecy (i.e. $K_C(p_{XYZ}) = K_D(p_{XYZ})$), then

$$K_D(p_{XYZ}) \geq E_{sq}(\rho^{AB}). \quad (28)$$

(b) If p_{XYZ} is UBI-PD (and hence reversible), then

$$K_D(p_{XYZ}) \geq E_F(\rho^{AB}). \quad (29)$$

(c) If p_{XYZ} has reversible secrecy and is semi-unambiguous, then

$$K_C(p_{XYZ}) = E_{sq}(\rho^{AB}) = K_D(\Psi^{ABE}) = K_D(p_{XYZ}). \quad (30)$$

(d) If p_{XYZ} has reversible secrecy, is semi-unambiguous and UBI-PD, then

$$\begin{aligned} K_C(p_{XYZ}) &= K_D(p_{XYZ}) = K_D(\Psi^{ABE}) = E_F(\rho^{AB}) \\ &= E_C(\rho^{AB}) = E_D(\rho^{AB}) = E_r(\rho^{AB}) = E_{sq}(\rho^{AB}) = H(J_{XY|Z}|Z). \end{aligned}$$

Proof. (a) By Theorem 3, if p_{XYZ} is reversible then there must be a channel $\bar{Z}|Z$ such that $p_{XY\bar{Z}}$ is block independent. In other words, there exists a decomposition

$$p_{XY\bar{Z}}(x, y|\bar{z}) = \sum_{j_{\bar{z}}} p(x|j_{\bar{z}}, \bar{z}) p(y|j_{\bar{z}}, \bar{z}) p(j_{\bar{z}}|\bar{z}) \quad (31)$$

where $p_X(\cdot|j_{\bar{z}}, \bar{z})$ and $p_X(\cdot|j'_{\bar{z}}, \bar{z})$ are disjoint distributions for $j_{\bar{z}} \neq j'_{\bar{z}}$, and likewise for Bob's conditional distributions. For each \bar{z} , define the local measurement channel acting on Alice's system

$$\omega \mapsto \Omega_A^{(\bar{z})}(\omega) := \sum_{j_{\bar{z}}} \sum_{\substack{x \text{ such that} \\ p(x|j_{\bar{z}}, \bar{z}) > 0}} \langle x|\omega|x\rangle |j_{\bar{z}}\rangle\langle j_{\bar{z}}|. \quad (32)$$

Let $\Omega_B^{(\bar{z})}$ be defined similarly for Bob's system.

We next consider the decomposition $|\Psi_{ABE}\rangle = \sum_z \sqrt{p(\bar{z})} |\varphi_z\rangle |z\rangle$, in which $\langle xy|\varphi_z\rangle = \sqrt{p(x, y|\bar{z})} e^{i\varphi_{xyz}}$. Note that $\rho^{AB} = \text{tr}_{\bar{Z}} \sigma^{AB\bar{Z}}$ where

$$\sigma_{AB\bar{Z}} := \sum_{\bar{z}} \sum_z p(z|\bar{z}) p(\bar{z}) |\varphi_z\rangle\langle\varphi_z| \otimes |\bar{z}\rangle\langle\bar{z}| = \sum_{\bar{z}} p(\bar{z}) \sigma_{(\bar{z})}^{AB} \otimes |\bar{z}\rangle\langle\bar{z}|. \quad (33)$$

On the state $\sigma^{AB\bar{Z}}$, we first dephase in the computational basis, and then apply $\Omega_A^{(\bar{z})} \otimes \Omega_B^{(\bar{z})}$ conditioned on \bar{z} . Doing so generates the state

$$\begin{aligned}\hat{\sigma}^{AB\bar{Z}} &:= \sum_{\bar{z}} p(\bar{z}) \sum_{x,y} p(x,y|\bar{z}) \Omega_A^{(\bar{z})}(|x\rangle\langle x|) \otimes \Omega_B^{(\bar{z})}(|y\rangle\langle y|) \otimes |\bar{z}\rangle\langle\bar{z}| \\ &= \sum_{\bar{z}} p(\bar{z}) \sum_{j_{\bar{z}}} p(j_{\bar{z}}|\bar{z}) |j_{\bar{z}}\bar{z}\rangle\langle j_{\bar{z}}\bar{z}|.\end{aligned}\tag{34}$$

Hence,

$$\begin{aligned}E_{sq}(\rho_{AB}) &\leq \frac{1}{2} \sum_{\bar{z}} p(\bar{z}) I(A : B)_{\sigma_{\bar{z}}^{AB}} \\ &\leq \frac{1}{2} \sum_{\bar{z}} p(\bar{z}) [S(\sigma_{\bar{z}}^A) + S(\sigma_{\bar{z}}^B)] \\ &\leq \frac{1}{2} \sum_{\bar{z}} p(\bar{z}) [S(\hat{\sigma}_{\bar{z}}^A) + S(\hat{\sigma}_{\bar{z}}^B)] \\ &= \sum_{\bar{z}} p(\bar{z}) H(J_{\bar{Z}}|\bar{Z} = \bar{z}) \\ &= K_D(p_{XYZ}).\end{aligned}\tag{35}$$

(b) If p_{XYZ} is UBI-PD then again by Theorem 3, we have $K_C(p_{XYZ}) = K_D(p_{XYZ}) = H(J_{XY|Z}|Z)$. Eq. (33) still holds in this case with $\bar{Z} = Z$, and σ_{ABZ} is obtained from $|\Psi_{ABE}\rangle$ by Eve dephasing in the computational basis. Block-independence of p_{XYZ} means that $S(\text{tr}_A |\varphi_z\rangle\langle\varphi_z|) = H(J_{XY|Z}|Z = z)$. Since $\{p(z), |\varphi_z\rangle\}$ provides a pure-state ensemble realizing ρ^{AB} , we see that $H(J_{XY|Z}|Z) \geq E_F(\rho^{AB})$.

(c) From Theorem 2 and Ref. [CEH⁺07], semi-unambiguous distributions are shown to satisfy the inequality $E_{sq}(\rho^{AB}) \geq K_D(\Psi_{qqq}^{ABE}) \geq K_D(p_{XYZ})$. Combining with part (a) gives the desired result.

(d) This follows from combining (c), (d) and Theorem 2 with the fact that $E_F(\rho^{AB}) \geq E_C(\rho^{AB}) \geq \max\{E_r(\rho^{AB}), E_{sq}(\rho^{AB})\}$.

□

Remark. While Theorem 6 (a) implies that Alice and Bob never gain an advantage over Eve when embedding their correlations into a quantum source, it is not difficult to construct distributions in which Eve gains a non-zero advantage in the quantum setting. This can be seen by the chain of inequalities in Eq. (35). In particular, whenever $\sigma_{\bar{z}}^{AB}$ is not pure the inequality will be strict. This will hold, for instance, for any distribution p_{XYZ} with a non-trivial channel $\bar{Z}|Z$ such that $p_{XY\bar{Z}}$ is UBI-PD.

5 Conclusion

In this paper we have considered the task of resource distillation in quantum and classical sources. Since secret key can be distilled from both quantum and classical states, a direct comparison can be made between the two scenarios. Quantum states that are diagonal in some fixed basis - such as ρ_{ccc} of Eq. (7) - lack coherence and are typically referred to as “classical” states since they possess the same entropic properties as classical probability distributions. However, as quantum objects, these states can undergo certain physical transformations that are impossible for classical states. We have shown that despite this enhanced dynamical ability, secret key distillation is equivalent

for a classical distribution and its incoherent quantum embedding. The situation is much different when the embedding takes the form of a coherent superposition. We have presented examples when quantum and classical key rates can be vastly different; sometimes it benefits Alice and Bob to have their correlations embedded in a quantum state, sometimes it benefits Eve. We have linked this investigation of quantum advantages to the problem of LOPC secrecy reversibility. By introducing different families of distributions that demonstrate secrecy reversibility, we are able to compute the entanglement and distillable key of the embedded quantum states. It is quite beautiful that notoriously difficult entanglement measures can be computed using exclusively a classical analysis of the states's underlying probability distribution. We hope this paper helps advance our understanding of the relationship between classical secrecy and quantum entanglement.

References

- [AC93] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography. i. secret sharing. *Information Theory, IEEE Transactions on*, 39(4):1121–1132, 1993. [doi:10.1109/18.243431](https://doi.org/10.1109/18.243431).
- [BB84] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. IEEE Press, Dec. 1984.
- [BBPS96] Charles H. Bennett, Herbert Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53(4):2046–2052, Apr 1996. [arXiv:quant-ph/9511030](https://arxiv.org/abs/quant-ph/9511030), [doi:10.1103/PhysRevA.53.2046](https://doi.org/10.1103/PhysRevA.53.2046).
- [BDSW96] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, Nov 1996. [doi:10.1103/PhysRevA.54.3824](https://doi.org/10.1103/PhysRevA.54.3824).
- [CEH⁺07] Matthias Christandl, Artur Ekert, Micha Horodecki, Pawe Horodecki, Jonathan Oppenheim, and Renato Renner. Unifying classical and quantum key distillation. In Salil P. Vadhan, editor, *Theory of Cryptography*, volume 4392 of *Lecture Notes in Computer Science*, pages 456–478. Springer Berlin Heidelberg, 2007. [doi:10.1007/978-3-540-70936-7_25](https://doi.org/10.1007/978-3-540-70936-7_25).
- [CFH15a] Eric Chitambar, Ben Fortescue, and Min-Hsiu Hsieh. Classical analog to entanglement reversibility. *Phys. Rev. Lett.*, 115:090501, Aug 2015. URL: <http://link.aps.org/doi/10.1103/PhysRevLett.115.090501>, [doi:10.1103/PhysRevLett.115.090501](https://doi.org/10.1103/PhysRevLett.115.090501).
- [CFH15b] Eric Chitambar, Benjamin Fortescue, and Min-Hsiu Hsieh. Distributions attaining secret key at a rate of the conditional mutual information. In Rosario Genaro and Matthew Robshaw, editors, *Advances in Cryptology – CRYPTO 2015*, volume 9216 of *Lecture Notes in Computer Science*, pages 443–462. Springer Berlin Heidelberg, 2015. URL: http://dx.doi.org/10.1007/978-3-662-48000-7_22, [doi:10.1007/978-3-662-48000-7_22](https://doi.org/10.1007/978-3-662-48000-7_22).
- [CH14] Eric Chitambar and Min-Hsiu Hsieh. Asymptotic state discrimination and a strict hierarchy in distinguishability norms. *Journal of Mathematical Physics*, 55(11), 2014. [doi:http://dx.doi.org/10.1063/1.4902027](https://doi.org/http://dx.doi.org/10.1063/1.4902027).

- [Chr06] Matthias Christandl. The structure of bipartite quantum states: Insights from group theory and cryptography. PhD Thesis, 2006.
- [CK11] Imre Csiszár and Janos Körner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, Cambridge, UK, 2011.
- [CLM⁺14] Eric Chitambar, Debbie Leung, Laura Maninska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about locc (but were afraid to ask). *Communications in Mathematical Physics*, 328(1):303–326, 2014. [doi:10.1007/s00220-014-1953-9](https://doi.org/10.1007/s00220-014-1953-9).
- [CW04] Matthias Christandl and Andreas Winter. “squashed entanglement”: An additive entanglement measure. *Journal of Mathematical Physics*, 45(3):829–840, 2004. [doi:10.1063/1.1643788](https://doi.org/10.1063/1.1643788).
- [CW05] M. Christandl and A. Winter. Uncertainty, monogamy, and locking of quantum correlations. *Information Theory, IEEE Transactions on*, 51(9):3159–3165, Sept 2005. [doi:10.1109/TIT.2005.853338](https://doi.org/10.1109/TIT.2005.853338).
- [DL70] E. Brian Davies and John T. Lewis. An operational approach to quantum probability. *Comm. Math. Phys.*, 17(3):239–260, 1970. [doi:10.1007/BF01647093](https://doi.org/10.1007/BF01647093).
- [GK73] P. Gács and J. Körner. Common information is far less than mutual information. *Problems of Control and Information Theory*, 2(2):149, 1973.
- [HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81(2):865, 2009. [doi:10.1103/RevModPhys.81.865](https://doi.org/10.1103/RevModPhys.81.865).
- [HHHO05] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.*, 94:160502, Apr 2005. [doi:10.1103/PhysRevLett.94.160502](https://doi.org/10.1103/PhysRevLett.94.160502).
- [HHHO09] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. *Information Theory, IEEE Transactions on*, 55(4):1898–1929, April 2009. [doi:10.1109/TIT.2008.2009798](https://doi.org/10.1109/TIT.2008.2009798).
- [HHT01] Patrick M. Hayden, Michał Horodecki, and Barbara M. Terhal. The asymptotic entanglement cost of preparing a quantum state. *J. Phys. A: Math. Gen.*, 34(35):6891, 2001.
- [Hua14] Yichen Huang. Computing quantum discord is np-complete. *New Journal of Physics*, 16(3):033027, 2014.
- [KKB11] Matthias Kleinmann, Hermann Kampermann, and Dagmar Bruß. Asymptotically perfect discrimination in the local-operation-and-classical-communication paradigm. *Phys. Rev. A*, 84(4):042326, Oct 2011. [doi:10.1103/PhysRevA.84.042326](https://doi.org/10.1103/PhysRevA.84.042326).
- [Mau93] U.M. Maurer. Secret key agreement by public discussion from common information. *Information Theory, IEEE Transactions on*, 39(3):733–742, 1993. [doi:10.1109/18.256484](https://doi.org/10.1109/18.256484).
- [OSS14] Maris Ozols, Graeme Smith, and John A. Smolin. Bound entangled states with a private key and their classical counterpart. *Phys. Rev. Lett.*, 112:110502, Mar 2014. [doi:10.1103/PhysRevLett.112.110502](https://doi.org/10.1103/PhysRevLett.112.110502).

- [Rai99] E. M. Rains. Rigorous treatment of distillable entanglement. *Phys. Rev. A*, 60:173–178, Jul 1999. [doi:10.1103/PhysRevA.60.173](https://doi.org/10.1103/PhysRevA.60.173).
- [RW03] Renato Renner and Stefan Wolf. New bounds in secret-key agreement: The gap between formation and secrecy extraction. In *Advances in Cryptology EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 562–577. Springer Berlin Heidelberg, 2003. [doi:10.1007/3-540-39200-9_35](https://doi.org/10.1007/3-540-39200-9_35).
- [VP98] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57(3):1619–1633, Mar 1998. [doi:10.1103/PhysRevA.57.1619](https://doi.org/10.1103/PhysRevA.57.1619).
- [Woo98] William K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80(10):2245–2248, Mar 1998. [doi:10.1103/PhysRevLett.80.2245](https://doi.org/10.1103/PhysRevLett.80.2245).

6 Appendix

6.1 Common Information

Let X and Y be random variables over finite sets \mathcal{X} and \mathcal{Y} respectively, with joint distribution p_{XY} . A **common partitioning of length t** for X and Y are pairs of subsets $(\mathcal{X}_i, \mathcal{Y}_i)_{i=1}^t$ such that

- (i) $\mathcal{X}_i \cap \mathcal{X}_j = \mathcal{Y}_i \cap \mathcal{Y}_j = \emptyset$ for $i \neq j$,
- (ii) $p(\mathcal{X}_i|\mathcal{Y}_j) = p(\mathcal{Y}_i|\mathcal{X}_j) = \delta_{ij}$, and
- (iii) if $(x, y) \in \mathcal{X}_i \times \mathcal{Y}_i$ for some i , then $p_X(x)p_Y(y) > 0$.

For every common partitioning, we associate a random variable $J(X, Y)$ such that $J(x, y) = i$ if $(x, y) \in \mathcal{X}_i \times \mathcal{Y}_i$. Note that each party can determine the value of J from their local information, and it is therefore called a **common function** of X and Y [GK73]. We will refer to the sets $\mathcal{X}_i \times \mathcal{Y}_i$ as the **blocks** of the given partitioning, and hence J is the “block number” random variable for the particular common partitioning.

A **maximal common partitioning** is a common partitioning of greatest length.

Proposition 1. *Every pair of finite random variables X and Y has a unique maximal common partitioning.*

With Proposition 1, we can speak unambiguously of *the* maximal common partitioning of two random variables X and Y . We let J_{XY} denote a **maximal common function** associated with the maximal common partitioning of XY ; i.e. $J_{XY}(x, y)$ is the number i for which $(x, y) \in \mathcal{X}_i \times \mathcal{Y}_i$ in the partitioning. Since J_{XY} is determined entirely from either X or Y , with a slight abuse of notation we will sometimes write $J_{XY}(x)$ (resp. $J_{XY}(y)$) if we wish J_{XY} to denote a function of x (resp. y). Note that J_{XY} is unique up to a relabeling of the blocks $\mathcal{X}_i \times \mathcal{Y}_i$. The entropic quantity $H(J_{XY})$ was identified by Gács and Körner as the **common information** of X and Y [GK73].

We now turn to the conditional form of common functions. For distribution p_{XYZ} , the variable $J_{XY|Z}$ is called a **maximal conditional common function** if $J_{XY|Z=z}$ is a maximal common function of the conditional distribution $p_{XY|Z=z}$. Explicitly, we have $J_{XY|Z}(x, y, z) = j$ if $(x, y) \in \mathcal{X}_j \times \mathcal{Y}_j$ for some fixed block labeling of the maximal common partitioning of $p_{XY|Z=z}$. Again, note that $J_{XY|Z}$ is unique for the distribution p_{XYZ} up to the choice of block labeling for each conditional distribution $p_{XY|Z=z}$. For the case when Alice and Bob are perfectly correlated (or when there is just one party), we also define $J_{X|Z} := J_{XX|Z}$.